I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Cybersecurity Policy as if "Ordinary Citizens" Mattered: The Case for Public Participation in Cyber Policy Making

PETER M. SHANE*

Were Gallup to poll the American people on the question, "What is cybersecurity?" it seems a fair guess that the following answers would be the most common: "Something to do with computer safety," "Preventing identity theft," and "I don't know." Few would likely refer to anything like "the body of technologies, processes and practices designed to protect networks, computers, programs and data [and the critical infrastructures on which they rely] from attack, damage or unauthorized access."[1] Yet, the likely poll answers and the more encompassing formal definition have something in common. All would probably suggest to the everyday citizen that the question, "How shall we pursue cybersecurity?" is a question best left to experts—preferably experts with computer science or engineering degrees.

The total abdication of cybersecurity policy to "experts," however, has been, and continues to be, a profound mistake. Given the ubiquity of computer networks and our reliance as a society on their integrity and robustness, the quality of cybersecurity is an issue that affects

* Jacob E. Davis and Jacob E. Davis II Chair in Law, Moritz College of Law, The Ohio State University.

[1] *What is Cybersecurity?*, WHATIS.COM (Dec. 17, 2010), http://whatis.techtarget.com/definition/cybersecurity.html (cited approvingly by the Securities and Exchange Commission in its guidance on corporate disclosures relative to cybersecurity); *see* SEC CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY, SEC. AND EXCH. COMM'N DIV. OF CORP. FIN. (2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

everyone's interests. Excluding the general public from any meaningful voice in cyber policymaking removes citizens from democratic governance in an area where our welfare is deeply implicated. Further, as the papers in this volume amply testify, the "technologies" and the "processes" entailed in cybersecurity are costly, likely requiring significant public investment.[2] Cybersecurity builds on "practices" that include routines and procedures in the hands of ordinary individual computer users.[3] Mobilizing citizen backing for the requisite public investment in cybersecurity, and even more for the common commitment to adopt responsible computing habits, will be substantially more difficult if people have virtually no understanding of what they are being asked to do or to support.

Finally, the concern over decision-making competence is easy to overstate. The design of cybersecurity involves technical choices requiring specialized competence, just as does the implementation of environmental policy, biomedical research policy, or, for that matter, counterinsurgency strategy in Afghanistan. But the design of cybersecurity also implicates a series of choices among competing values and priorities that are the ordinary stuff of politics. The lay public's inability to address strictly technical or expert questions does not mean it is incompetent to weigh competing policy answers to the general question, "What should the government do?"[4]

Indeed, I would argue that an administration explicitly committed to unprecedented levels of both transparency and collaboration[5] should regard cybersecurity as offering an ideal opportunity to engage the public more meaningfully in policy deliberation than has so far been the American norm. Models abound, both in other nations' use of citizen consultations to involve the public in technology-related policy making and in U.S. experience with citizen consultation in

---

[2] For partial data on the government budgets allocated for cybersecurity, see Mark D. Young, *Cyber Operational Relationships in the United States Government*, 8 ISJLP 270 (2012).

[3] ORG. FOR ECON. CO-OPERATION AND DEV., COMPUTER VIRUSES AND OTHER MALICIOUS SOFTWARE: A THREAT TO THE INTERNET ECONOMY 151 (2009).

[4] *See* JAMES S. FISHKIN, WHEN THE PEOPLE SPEAK: DELIBERATIVE DEMOCRACY AND PUBLIC CONSULTATION 118-19 (2009).

[5] Memorandum on Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009) ("My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government.").

environmental decision making.[6] Not only do such models offer the prospect of improving our cyber policy posture through public engagement, but meaningful citizen engagement in this area of complex decision making could provide a pivotal model for how to deepen the meaning of citizenship in the digital age.

In Part I of this essay, I will revisit the other contributions to this volume to illustrate the range of policy tradeoffs that could sensibly be opened up for public discussion. In Part II, I will discuss what ought to be the aims behind any project to incorporate public deliberation into cyber policymaking. Part III will review models of public input that could give lay citizens a meaningful recommending voice in the formulation of government cyber policy, and suggest the model best suited to meet the aims set forth in Part II. Part IV discusses the typical objections to genuinely collaborative public input, but argues that cyber policy provides an exceptional opportunity to set a precedent for the institutionalization of collaborative public involvement in policy making more generally.

I. CYBER POLICY AND PUBLIC VALUES

The obvious threshold difficulty in creating a cybersecurity regime that resembles a "kinetic world" security regime is one of attribution: it is often exceedingly difficult, if not impossible, to discern the source of aggressive efforts to exploit the vulnerabilities of cyber systems.[7] That fact directly implies that any cyber policy discussion is sooner or later going to focus on attribution, and set up a familiar debate between champions of security and champions of privacy. Before even contemplating how public input might be useful to that debate, however, it is worth emphasizing that the typical security-versus-privacy frame barely scratches the surface in terms of what Americans have at stake in the framing of cyber policy.

As a starting point, it is useful to note the contrast that the National Research Council (NRC) has delineated between "cyber attack" and "cyber exploitation." The former term "refers to the use of deliberate actions . . . to alter, disrupt, deceive, degrade, or destroy

---

[6] *See, e.g.*, Johs Grundahl, *The Danish Consensus Conference Model*, *in* PUBLIC PARTICIPATION IN SCIENCE: THE ROLE OF CONSENSUS CONFERENCES IN EUROPE 31, 31-40 (Simon Joss & John Durant eds., 1995).

[7] *See* JEFFREY HUNKER, CREEPING FAILURE: HOW WE BROKE THE INTERNET AND WHAT WE CAN DO TO FIX IT 84-85 (2010); NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 20 (William A. Owens et al. eds., 2009).

adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[8] An attempt to shut down an urban transportation system by disrupting the computer programs that govern its operations would be such a cyber attack. By contrast, cyber exploitation "is an intelligence-gathering activity rather than a destructive activity."[9] Its aim is to secure unauthorized access to confidential information, while allowing the computer system on which that information resides to run normally. Cyber exploitation is more like espionage than warfare. Yet, as the NRC notes, "[c]yber attack and cyber exploitation are often conflated in public discourse," increasing the likelihood that policy discussions about cyber exploitation are distorted by the kinds of public anxiety stirred up by cyber attack scenarios.[10]

Policy making with regard to potential cyber attack—from both an offensive and defensive posture—is rife with the sorts of value questions on which informed citizens can make meaningful contributions. Not least among them, as this volume well documents, is the determination of appropriate responsibilities to be assigned to civilian and military authorities in responding to a cyber attack. Mark Young has sketched the ongoing evolution among federal entities, both military and civilian, of a series of operational relationships in cyber defense that he still regards as insufficiently mature to meet the current cyber threat.[11] He identifies the debate about the Defense Department's appropriate role in protecting civilian networks as one that should be discussed "openly and frequently."[12]

Other papers testify to the importance of this debate. As analyzed by information scientist Martin Libicki, the seemingly reflexive characterization of cyber space as a new military domain—reinforced by the formal creation within the military of a cyber "command"—runs the risk of skewing the emergence of cyber doctrine in ways that are counterproductive for developing both strategy and tactics.[13] Yet, as Terrence Kelly and Jeffrey Hunker attest,

---

[8] NAT'L RESEARCH COUNCIL, *supra* note 7, at 10 -11 .

[9] *Id.* at 1.

[10] *Id.* at 32.

[11] Young, *supra* note 2.

[12] *Id.* at 299.

[13] Martin Libicki, *Cyberspace Is Not a Warfighting Domain,* 8 ISJLP 321 (2012).

there seems little doubt that the greatest reservoir in the federal government of technical expertise regarding cyber attack sits with the Department of Defense, on both the military and civilian sides.[14] What then is to be done in pursuit of the levels of efficiency, effectiveness, transparency, and accountability that the public might appropriately expect in this realm? How to organize multiple players to achieve these competing goods is a subject that an informed public can and should rationally discuss.

Critical value questions also attend the prospect of launching cyber attacks from the U.S. The NRC has noted the imperfect match between the nature of cyber conflict and the legal regime that attends kinetic war making—the international laws of armed conflict, the United Nations Charter, and the conventional *modus vivendi* between Congress and the executive branch regarding the initiation of military conflict generally.[15] There is no reason why the public should be excluded from meaningful discussions about how best to analyze potential cyber attack scenarios within the existing framework, and what new rules or doctrines need to be evolved to take account of the new world of cyber weapons. This is especially so because, as the NRC states:

> U.S. cyber attacks that are directed against globally shared infrastructure supporting the private sector might have deleterious "blowback" effects on U.S. private sector entities. Such effects might be direct, in the sense that a U.S. cyberattack might propagate to harm a U.S. firm. Or they might affect the supply chain of a U.S. firm—a node in Zendia might support communications between a key U.S. firm and a supplier firm in Ruritania as well as military communications in Zendia, and a disabling cyberattack on that node might leave the U.S. firm without the ability to order goods from the Ruritanian firm.[16]

In other words, U.S.-launched cyber attacks would likely risk serious ramifications for ordinary Americans, as well as for our government

---

[14] Terrence K. Kelly & Jeffrey A. Hunker, *Cyber Policy—Institutional Struggle in a Transformed World*, 8 ISJLP 210 (2012).

[15] *See* NAT'L RESEARCH COUNCIL, *supra* note 7, at 239-92.

[16] *Id.* at 47.

and for the international targets of our attacks. The public should be afforded some form of democratic input before bearing those risks.

In this volume, Herbert Lin, a distinguished computer scientist and major contributor to the NRC study, explains that decision makers involved in cybersecurity are now working with scant information about both the intentions and technical capacities of likely cyber aggressors, thus prompting analysts to plan around worst-case scenarios.[17] He points out that, "[i]n the absence of metrics that tie investment to capability (a difficult problem that has bedeviled the cybersecurity community for forty years and remains unsolved today)," analysts are left to make judgments on cyber preparedness based on significantly subjective estimates of what is reasonable.[18] There is no reason to exclude the public from such a discussion. This is especially so, given that, as Dr. Lin elaborates, strategic responses to cyber attack could assume two quite different forms: "passive" early warning and defensive measures, and measures to "enhance rapid recovery . . . and resilience . . . to deploy backup or alternative capabilities; and to train organizations that might be affected by the loss of cyber functionality to work without it."[19] Dr. Lin concludes that worst-case scenarios, if reasonable, would most likely prompt emphasis on the latter forms of response.[20] Yet, for all the public knows, millions of public dollars are being pumped into warning and defense measures that are likely inadequate to respond to the very scenarios prompting their development.

Of course, life is yet more complex because, as many papers in this volume reflect, much of the digital infrastructure that supports critical functions in U.S. civilian life is actually in the hands of private firms.[21] As a consequence, it is impossible to imagine any plausible defense against cyber attack that does not significantly involve the private sector. In May 2011, the Obama Administration made a proposal for new legislation that would motivate private sector firms

---

[17] Herbert Lin, *Thoughts on Threat Assessment in Cyberspace*, 8 ISJLP 337 (2012).

[18] *Id.* at 353.

[19] *Id.*

[20] *Id.*

[21] *E.g.*, Mark MacCarthy, *Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry*, 8 ISJLP 242 (2012).

to improve their security preparedness.[22] Under the Administration proposal, the Department of Homeland Security would:

> [W]ork with industry to identify the core critical-infrastructure operators and to prioritize the most important cyber threats and vulnerabilities for those operators. Critical infrastructure operators would develop their own frameworks for addressing cyber threats. Then, each critical-infrastructure operator would have a third-party, commercial auditor assess its cybersecurity risk mitigation plans. Operators who are already required to report to the Security and Exchange Commission would also have to certify that their plans are sufficient. A summary of the plan would be accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify a framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial auditors.[23]

Ink had barely dried on the proposal before the U.S. Chamber of Commerce broadcasted its opposition. The Chamber immediately declared: "Layering new regulations on critical infrastructure will harm public-private partnerships, cost industry substantial sums, and not necessarily improve national security."[24] According to the

---

[22] *See* Letter from Jacob J. Lew, Director, Office of Management and Budget, to Hon. John Boehner, Speaker of the House of Representatives (May 12, 2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-letters-to-congress-house-signed.pdf (forwarding the proposal. The actual proposal is available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf (last visited Mar. 10, 2012)).

[23] THE WHITE HOUSE, FACT SHEET: CYBERSECURITY LEGISLATIVE PROPOSAL 3 (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf.

[24] Siobhan Gorman, *Cybersecurity Plan Faulted*, WALL ST. J. (May 27, 2011), http://online.wsj.com/article/SB10001424052702303654804576345772352365258.html (quoting U.S. Chamber of Commerce, White House Security Proposal Moving from Risk Management to Regulatory Overreach (May 2009)).

Chamber, compliance with external audits would be "costly and time consuming, particularly for small businesses."[25] This cost-benefit analysis, however, dramatically poses exactly the kind of tradeoff on which a democratic society should have a broad-based dialogue. It is certainly questionable whether private-public partnerships are likely to improve security if the government has no significant leverage to elicit cooperation from its private sector "partners." The Chamber's point of view might or might not prove sound, but it ought not represent the only public voice in a critical policy debate.

The issues on the cyber exploitation, or information security, side are no less value-laden or ripe for public debate. As Mark MacCarthy's paper points out, our financial systems constitute an important domain in which to consider the appropriate respective roles for government and the private sector.[26] Dr. MacCarthy argues that the proper locus for the legal imposition of security requirements is at the federal, not the state level, and that mandatory requirements ought to be limited to general principles, not specific implementation steps.[27] He also argues against the utility of private rights of action against financial firms that underinvest in cybersecurity.[28] These are entirely plausible positions; the preference for performance standards over requirements for specific technologies now has a distinguished pedigree in the literature—and politics—of regulatory reform.[29] Yet, efforts to enact sensible federal cybersecurity legislation appear to be chronically stalled because the "deliberative process" has been hijacked by special interests and partisan acrimony.[30] Bringing the public into the debates about both general regulatory philosophy and specific legislative proposals might help Congress and federal agencies break free of the inertia of inside-the-Beltway politics-as-usual.

---

[25] *Id.*

[26] MacCarthy, *supra* note 21.

[27] *Id.* at 269–71.

[28] *Id.* at 270.

[29] *See, e.g.*, Exec. Order No. 12866: Regulatory Planning and Review, 58 Fed. Reg. 51735, 51736 (Oct. 4, 1993) ("Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt.").

[30] Aliya Sternstein, *Political and Industry Wrangling Likely Will Delay Cybersecurity Reforms*, NEXTGOV.COM (Sept. 26, 2011), http://www.nextgov.com/nextgov/ng_20110926_1907.php.

Because of the difficulty of attribution mentioned earlier, debates concerning the nature and resolution of privacy-security tradeoffs permeate discussions of both cyber attack and cyber exploitation.[31] Greg Nojeim's paper highlights a handful of proposals that privacy advocates have long challenged, including grants of government authority to block or limit communications on private computer networks, expansion of the government's monitoring authorities over private networks, and the facilitation of electronic surveillance by mandating technology designs that enable wiretapping.[32] Jeffrey Hunker, however, is advancing a proposal arguably further reaching than any of these: the engineering of a new Internet that would build security into its architecture, thus facilitating attribution.[33] The proposal is a fascinating one because the stakes are so high. On one side, there would undoubtedly be concerns not only for the resulting impacts on privacy, but also for the magnitude of public investment it would take to engineer a new Internet and for the possibility that increasing network management at a new Internet's "core" would limit the Internet's power as a platform for innovation and universal connection.[34] On the other hand, Dr. Hunker holds out the prospect that a new Internet would enable governments, businesses, and individuals all to engage in data and communication activities with greater confidence, efficiency, and security—virtues that could significantly boost both the economy and our social and political life more generally.[35]

A new Internet could be a great idea—or a terrible one—but the public is never likely to focus on it unless there is a meaningful, structured opportunity for informed citizens to learn about and express themselves regarding the possibilities. Those firms currently invested in owning or providing services over the current Internet

---

[31] Ellen Nakashima, *White House, NSA weigh cybersecurity, personal privacy*, WASH. POST, Feb. 27, 2012 at 1, *available at* http://www.washingtonpost.com/world/national-security/white-house-nsa-weigh-cyber-security-personal-privacy/2012/02/07/gIQA8HmKeR_story.html.

[32] Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come—And Shouldn't*, 8 ISJLP 408 (2012).

[33] *See generally* HUNKER, *supra* note 7, at 204-23.

[34] *See generally* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010) (arguing the importance of the original architecture of the Internet to its power as a platform for innovation).

[35] HUNKER, *supra* note 7, at 208.

likely constitute a sufficiently weighty inertial force to prevent serious consideration of so ambitious a proposal within our usual official public policy forums. Given the magnitude of cyber threat that contributors to this volume have identified vis-à-vis our current Internet, however, this is a debate worth having—a debate informed by, but not limited to, experts in computer science, engineering, information technology management, and public administration (on both the civilian and defense sides).

II. THE AIMS OF PUBLIC ENGAGEMENT IN CYBER POLICY

The norm of public engagement is deeply embedded in the laws and institutions of Western governments, but the precise mechanisms of public engagement are highly varied. In general, the concept "covers a broad range of interactions between government and civil society to design, implement, and evaluate policies."[36] Available models include at least the following:[37]

- Referenda
- Public surveys
- Formal notice and comment filing opportunities
- Blogs
- Wikis
- "Serious games" and online simulations
- Public hearings

---

[36] FRANS H.J.M. COENEN, PUBLIC PARTICIPATION AND BETTER ENVIRONMENTAL DECISIONS: THE PROMISE AND LIMITS OF PARTICIPATORY PROCESSES FOR THE QUALITY OF ENVIRONMENTALLY RELATED DECISION-MAKING 3 (Frans H.J.M. Coenen, ed., 2008).

[37] This list borrows from: *id.* at 15; FISHKIN, *supra* note 4; THOMAS DIETZ & PAUL C. STERN, PUBLIC PARTICIPATION IN ENVIRONMENTAL ASSESSMENT AND DECISION MAKING 49 (2008); and MATT LEIGHNINGER, IBM CTR. FOR THE BUS. GOV'T, USING ONLINE TOOLS TO ENGAGE—AND BE ENGAGED BY—THE PUBLIC (2011), *available at* http://www.businessofgovernment.org/sites/default/files/Using%20Online%20Tools%20to%20Engage%20The%20Public_0.pdf.

- Consensus conferences
- Mediation
- Regulatory negotiation
- Citizen juries
- Planning cells
- Citizen advisory committees
- 21st Century "Town Halls" (as sponsored by AmericaSpeaks)
- Deliberative polls

If cyber policy making is to involve public participation, a choice among these models must be made. Any sensible design choice must be guided by the aims that this particular public participation project would be intended to accomplish.

The aims most often advanced in connection with public participation are threefold: public education and mobilization, better quality decisions, and enhanced decision-making legitimacy.[38] In the cyber realm, the aims of public education and mobilization seem highly salient. The issues are complicated. The tradeoffs are subtle. Greater public knowledge is a likely prerequisite to the kinds of behavioral change among ordinary users that would enhance network security. Greater public knowledge is also quite likely a prerequisite to mobilizing political support for the levels of public investment required to advance cybersecurity. It would thus seem imperative to design public participation opportunities in the cyber policy realm to maximize public awareness and knowledge acquisition.

What "better" decision making consists of in the cyber (or any other) realm is ambiguous.[39] In terms of efficiency, it might seem obvious that the best cybersecurity decisions would be those that achieve the most appropriate levels of network and critical infrastructure security at the least cost. It may simply prove

---

[38] COENEN, *supra* note 36, at 2.

[39] *Id.* at 3-6.

impossible, however, to ever make such an assessment persuasively. Additionally, the goal of efficiency needs to be weighed in conjunction with considerations of distributive equity. A least-net-cost solution would likely seem less attractive if the costs are unduly borne by any one segment of the affected public.

It seems reasonable then, as a second-best approach, to judge the quality of decisions at least in part by inputs that are observable and thus manageable. For example, were decisions based on a shared understanding of the problem under examination? Was the most current and reliable information brought to bear? Did decision makers have the benefit of well-informed arguments for contending positions? Were efforts made to curb the kinds of decisional bias that can skew group interaction? Were efforts made to ensure that recommendations would not disproportionately burden persons or interests who went unrepresented in the decisional process? Given these criteria, we should want a model for public participation that makes the development of a coherent, shared understanding of the issue most likely, and which brings to the forefront the best information and the strongest arguments from a truly inclusive group.

As for enhancing legitimacy, three factors would seem to loom largest. The first is whether the deliberation was representative of the affected public which, in the cyber domain, is really everyone. The second is whether there was transparency and balance in the development and presentation of the scientific or other technical information that set the foundation for deliberation. The third is whether there is a credible commitment among policy makers to take the consequences of public participation into serious account. This need not be a commitment to do what a majority of participants prefer, but it should be at least a commitment to explain ultimate decisions publicly, including reasons for not acting in concert with the public deliberation should the relevant decisions actually go that way.[40]

Translating the general values associated with public participation into appropriate objectives for a public participation initiative on cybersecurity thus produces the following specifications. The project should:

---

[40] *See* DIETZ & STERN, *supra* note 37, at 99; FISHKIN, *supra* note 4, at 150-58.

- Aim at maximizing informed public awareness;
- Engage a significant representative sample of Americans in policy deliberation;
- Facilitate discussions aimed at generating a common, coherent understanding of the problems under consideration;
- Involve the most reliable current information;
- Publicize the sources of information being discussed and the processes by which that information was produced;
- Expose participants to strong arguments for all contending positions;
- Deploy best practices in terms of reducing the influence of group processes that reduce the quality of deliberative outcomes; and
- Entail a commitment by relevant policy makers to take the recommendations of the public participants into serious account, including a commitment to offer public reasons for not following any recommendations that the majority of public deliberators favor.

This list of objectives appears yet more appropriate because of what Jeffrey Hunker and Terrence Kelly argue in their introduction are the prerequisites for success in the formulation and implementation of public policy. Distilling from their own government experience, they identify the four foundational requirements as:

1. Clear statements of what the policy is to achieve (goals) and acceptable approaches to achieving these goals, derived from consensus among key stakeholders;
2. Authorities that permit government to act;

3. Resources—both fiscal and human—to implement the proposed policy; and

4. Government organizations that have the capabilities (e.g., organizational structure, skills, knowledge, relationships within government and with the private sector), and capacity (i.e., resources—mostly people and fiscal resources) required to implement policy.[41]

Public participation alone cannot yield all of these elements. Yet, it is easy to imagine designing a process aimed explicitly at Point 1. If the process works well, public support for developing Points 2 through 4 could significantly increase. Government agencies should thus view public participation not only as a tool for policy development per se, but also as providing an opportunity for the kind of public education and mobilization that can yield increases in the human, fiscal and legal resources that are essential to agency success.

III. MODELS FOR PUBLIC INPUT

Requirements for public input in connection with public policy making are hardly new to the United States. Public hearings are part and parcel of the decision making process for agencies at every level of government. Federal and state governments typically require opportunities for public comment to accompany significant proposals for new administrative regulations.[42] These opportunities, while taken seriously by agencies at the federal level at least, suffer from obvious deficiencies. The pattern of public participation is uneven, and the connection between public input and policy outcomes uncertain.[43] The Obama Administration has worked to expand public input opportunities, chiefly through online sites for policy discussion, proposal review, and petitioning.[44] It has even experimented with

---

[41] Kelly & Hunker, *supra* note 14.

[42] *See, e.g.*, 5 U.S.C. § 553(c) (2006) (requiring that federal administrative agencies provide public comment opportunities for most agency rule making).

[43] *See generally* Cornelius M. Kerwin & Scott R. Furlong, RULEMAKING: HOW GOVERNMENT AGENCIES WRITE LAW AND MAKE POLICY (4th ed. 2010).

[44] Peter M. Shane, *Online Consultation and Political Communication in the Era of Obama, in* CONNECTING DEMOCRACY: ONLINE CONSULTATION AND THE FLOW OF POLITICAL COMMUNICATION 1 (Stephen Coleman & Peter M. Shane eds., forthcoming Dec. 2012). The

public collaboration in policy drafting via wiki technologies.[45] None of these models, however, is well-designed to meet the objectives identified above as appropriate for a public participation project on cybersecurity. None is representative. None is structured to maximize the quality of information input or to facilitate fully engaged deliberation. None is consciously designed to reduce the influence of social and cognitive processes that degrade the quality of decision making.

A well-entrenched and more meaningful example of government initiative to engage the public in deliberations on technology policy is the Danish consensus conference.[46] Under this model, the Danish Board of Technology (DBT) organizes formal meetings between panels of experts and lay panels of concerned citizens, which result in reports and recommendations by the lay panels that are directed to the relevant decision makers, as well as to the public more generally. Each such conference lasts for three days and is open to the public, although panel participants commit to two additional preparatory weekends, as well as additional time reading briefing materials.

Significant responsibility for staging a consensus conference rests with a project manager, who is an employee of the DBT's Secretariat. The project manager works with the DBT to create a steering committee for the conference, to arrange for the selection of experts, and to recruit both the lay panel members and a professional lay facilitator. Members of the public must apply to be considered for lay panel membership, but the project manager and steering committee select their ultimate group of ten to fourteen deliberators to be diverse in outlook and according to a variety of socio-economic criteria.

It is the responsibility of the steering committee to determine how information will be assembled into briefing materials for participants. In order to assist in gathering ideas, the steering committee may provide for a written or live hearing among interested stakeholders. The project manager may ultimately be asked to produce the conference briefing paper from existing research sources, or to hire an external writer to do the work. Responsibility for final approval of the briefing materials rests with the steering committee.

Obama White House e-petitioning site called, "We the People," appears at https://wwws.whitehouse.gov/petitions (last vitisted Mar. 10, 2012).

[45] Shane, *supra* note 44, at 10-11.

[46] Details of the Danish consensus conference process are drawn from Grundahl, *supra* note 6.

The preparatory weekends held prior to the actual conference are devoted chiefly to the lay panel's formulation of questions to be posed to the expert panel. The lay panel also expresses its preferences for the kinds of experts from whom it wishes to hear. The first day and a half of the actual consensus conference is devoted to expert presentations that are responsive to the panel's questions, after which the lay panel prepares its final document. The lay panel presents its report on the third day, at which point the experts and the public audience have the opportunity to direct questions and reactions to the lay panel. The reports can become influential in a way that belies each panel's small size. That is because the media generally provides strong coverage of the conferences, which may, in turn, further motivate policy makers' interest in appearing responsive.

Although institutionalized public outreach of this sort is commendable, the consensus conference model would not be ideal for federal cybersecurity deliberations in the United States. Most obviously, it is not a reliably representative process. But just as worrisome, its information gathering protocol is probably not as well suited to a national community that is far larger and more diverse than Denmark. To put the matter bluntly, having a three-to-five-member committee of government appointees and their designated project manager put together the briefing materials on which the deliberation is based is not likely to inspire trust in the deliberative outcome among a polity as polarized and often as cynical as the American public.

Domestically, the science-infused policy arena in which public participation is most often incorporated is decision making involving the environment. Such participation may take the form of public meetings and hearings, advisory committees, various forms of mediation, or negotiated rulemaking. Although participants regard the last of these models—negotiated rulemakings[47]—as producing a variety of positive outcomes, including better-quality decisions,[48] the model is not likely to work any better than the consensus conference for the cybersecurity policy domain. Negotiated rulemaking is premised on a finding that there exist only "a limited number of identifiable interests that will be significantly affected by the rule"[49] in

---

[47] The process was created by the Negotiated Rulemaking Act, 5 U.S.C. §§ 561-570(a) (2006).

[48] DIETZ & STERN, *supra* note 37, at 78.

[49] 5 U.S.C. § 563(a)(2)(2006).

question, and usually on the adequacy of a committee comprising no more than twenty-five members to represent those interests.[50] For the overarching cyber policy questions facing the U.S., these premises are patently unrealistic.

A form of structured interaction among lay citizens and experts that responds directly to the mismatch between the most appropriate roster of cyber policy participation objectives and the design of either consensus conferences or negotiated rulemaking is "deliberative polling," pioneered by philosopher and political scientist James Fishkin.[51] When a sponsor entity decides to launch a Deliberative Poll (DP), it typically works with an outside neutral consultant—frequently Professor Fishkin himself—to create an advisory committee of stakeholders. The consultant arranges for one or more researchers to assemble briefing materials, which are vetted by the stakeholders. The aim is not a consensus document—if consensus were possible, no deliberation would likely be required—but a fair presentation of all competing perspectives. The representatives of competing interests in the advisory group must all agree that the briefing materials fairly represent their respective points of view.

Participants in a DP are chosen by random sampling, which is the key factor that differentiates Deliberative Polling from other models.[52] A random sample is assembled from the relevant jurisdiction—from local to national—that is large enough to yield 150 to 300 or more participants for the actual face-to-face interaction. All individuals targeted for potential recruitment participate in an initial survey prior to being invited to participate in the face-to-face discussions. This method allows a careful comparison of the group that participates and the group that declines. It assures that the representativeness of the original sample is not lost because the group that agrees to participate is distinctively different in attitudes or demographics from the overall random sample. If the sponsors of a deliberation judge that the relevant population includes a subgroup whose participation is critical, but which is too small in size to be assured any representation at all in a random sample—for example, Aboriginals in Australia participating in a national deliberation on policy toward Aboriginals[53]—that group may be oversampled to ensure some

---

[50] 5 U.S.C. § 565(b)(2006).

[51] *See generally* FISHKIN, *supra* note 4.

[52] *See generally id.* at 25-28, 111-19.

[53] *Id.* at 161-63.

ultimate presence. In contemplating any potential national DP on cyber policy, however, it seems unlikely that any oversampling would be necessary. The deliberating group could be genuinely representative.

The survey respondents who accept the invitation for a weekend of face-to-face deliberation are compensated modestly for their participation. Upon arrival at the deliberation site, they are randomly assigned to small groups of ten to fifteen members, each of which is led by a trained neutral moderator. The small groups start by discussing the briefing materials and identifying those issues or concerns they feel the materials do not sufficiently address. These discussions yield questions from each group that are then posed to a group of competing experts and policy makers during a plenary session. After one or two rounds of such discussions, the small groups get a final opportunity to discuss the issue that is actually the focus of the deliberative poll. Finally, the participants re-take the confidential questionnaire they were given at first contact, in order to determine if and in what ways the experience of deliberating affects knowledge acquisition and opinion.

What emerges from a DP is a particular kind of democratic recommendation. It is not a consensus —unlike a jury, the DP participants need not reach a united verdict.[54] What policy makers learn from the DP is what a random sample of Americans thinks about a problem if they are given a fair opportunity to understand the issues and asked their opinion in a context in which they perceive their contributions to be potentially consequential. In his 2009 book based, in part, on nine nation-level DPs conducted in the U.S. and abroad between 1995 and 2004, Professor Fishkin cites consistent and significant evidence of attitude change as a result of the deliberative experience.[55] Deliberators experience substantial knowledge gains with regard to both the issue in contention and the positions of contending parties. Deliberation moves its participants towards a more rational ordering of their own preferences. And, quite critically, DPs have attracted a level of media attention that can affect a broader public dialogue and attract the serious attention of policymakers.

Of course, although a deliberative body of 300 sounds significantly more inclusive than a consensus conference of fifteen or a negotiated rulemaking committee of twenty-five, it may still seem too small a sample of engaged citizens to fulfill the aim of maximizing informed

---

[54] *Id.* at 129, 132.

[55] *Id.* at 134.

public awareness. Media, however, can have a huge amplifying effect, especially if arrangements are made beforehand to document the deliberations through film, as well as text, and make the conversation available to the public at large. It would also be possible to supplement a face-to-face DP with an online version of a DP that could substantially multiply the number of citizens directly involved.[56]

It may be called into question, of course, whether even deliberations as carefully structured as DPs will yield sound decisions based on genuinely representative input. As summed up by Cass Sunstein, deliberating groups "typically suffer from four problems" undermining decisional soundness: "They amplify the errors of their members. They do not elicit the information that their members have. They are subject to cascade effects, producing a situation in which the blind lead the blind. Finally, they show a tendency to group polarization, by which groups go to extremes."[57] Other democratic theorists who have written about deliberation express concern about the prospect that deliberative outcomes will be skewed by variously advantaged subgroups who, by virtue of their status or manipulative skills, will dominate group discussions.[58]

Beyond its capacity to catalyze public awareness and to facilitate productive discussion around a balanced presentation of contending positions, however, deliberative polling has also shown its value by reducing the influence of group processes that reduce the quality of deliberative outcomes. As reported by Fishkin, and as substantiated by empirical study of his deliberating groups, DPs do well at avoiding these problems.[59] Three features of the DP appear critical in this regard. First, DP groups are not solely dependent on their members' knowledge to inform group discussion.[60] Discussions are framed by carefully vetted and balanced presentations of well-informed and competing views. Discussants are urged to consider what further information they need to reach their conclusions, and are given the opportunity to pose their questions to experts from outside their groups. Second, the groups are conducted by trained moderators, one

---

[56] *Id.* at 170-75.

[57] CASS R. SUNSTEIN, INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE 75 (2006).

[58] *See, e.g.*, IRIS MARION YOUNG, INCLUSION AND DEMOCRACY 52-57 (2000); Lynn M. Sanders, *Against Deliberation*, 25 POLITICAL THEORY 347 (1997).

[59] FISHKIN, *supra* note 4, at 130.

[60] *Id.* at 132.

of whose primary tasks is to prevent domination.[61] A study of five U.S. DPs found "that no particular gender, race, or demographic dominates deliberations," and no pattern of opinion convergence towards the initial positions held by members of higher-status groups—whites, men, high-income participants, and the well-educated.[62] This strongly suggests the success of the moderated structure. Finally, unlike juries or consensus panels, participants in DPs are not required to reach a unanimous verdict of any sort. Hence, there is simply less social pressure to converge on a single point of view. Fishkin's analysis of fifteen DPs studied for polarization effects found that the groups were just as likely to converge to the mean point of view as to push away from it in an extreme direction. Although there was some modest evidence of a homogenization of group views,[63] it seemed as likely to be the outcome of the thoughtful weighing of competing alternatives as the product of "groupthink."[64]

Perhaps the greatest disadvantage to a DP on cyber policy would be the expense entailed in assembling a genuinely representative sample. There are variants of the DP experienceBritish Columbia's Citizen Assembly, which proposed a series of electoral reforms in that province, is likely the most famous[65]—that strongly resemble DPs in some of their elements, but are more tolerant of self-selection in the recruitment of deliberators. It might be argued that the lengths to which DPs go to provide guarantees of representativeness adequate to assure social scientists of their integrity might be more rigorous than necessary. Some mixture of demographic screening and the acceptance of volunteers might be enough to generate the kind of national microcosm that would appear both to relevant policy makers and to the general public to be representative enough to be worthy of serious attention. The American public, however, is currently both so polarized—as are its policy makers—and so distrustful of public institutions that the extra care necessary to insure the

---

[61] *Id.*

[62] *Id.* at 130.

[63] *Id.* at 131-132.

[64] *Id.* at 132.

[65] *Making Every Vote Count: The Case for Electoral Reform in British Columbia*, BRITISH COLUMBIA CITIZENS' ASSEMBLY ON ELECTORAL REFORM (2004), http://www.citizensassembly.bc.ca/resources/final_report.pdf.

representativeness of a deliberative forum might prove a sound investment in eliciting public confidence in the process. Among the available models for public participation in policy making, deliberative polling or its equivalent would seem most likely to fulfill the appropriate objectives for public participation in the cyber policy realm.

IV. THE CASE FOR COLLABORATIVE CYBER POLICY MAKING

The U.S. currently faces cyber policy issues that raise questions of value and general direction susceptible to intelligent discussion by non-specialists. Public participation has long been linked to a series of benefits for governance that are salient in the realm of cyber policy. Models of lay deliberation exist that are well designed to achieve those benefits. Powerful questions remain, however, about the role of a deliberative public in making government policy and whether public participation—even if attractive in principle—can be designed effectively to ward off predictable sources of frustration and poor quality.

The case for public participation in policy making has both normative and instrumental aspects. The core normative proposition is that genuinely democratic governance must entail public participation. With the exception of purely procedural theories, in which democracy means little more than institutionalized electoral competition under fair conditions, contemporary political theorists have coalesced around what the NRC has called "a remarkable consensus" on three key elements of democracy: political equality, popular sovereignty, and human development.[66] By definition, political equality entails the right of every citizen to participate in making public policy. Popular sovereignty proposes that democratic citizens be governed only by laws to which they give consent in some meaningful way. Human development captures the idea that democratic participation not only allows citizens to promote their interests, but represents "an important means through which they come to understand their interests in the first place and how those interests relate to and depend on those of other citizens."[67] Democracy, in this last sense, is a system of "experiential learning." There is thus a direct link between citizen involvement in policy

---

[66] DIETZ & STERN, *supra* note 37, at 46.

[67] *Id.* at 47.

making and each feature of governance that is now regarded as foundational to democracy.

It is understandable however, that policy makers—both elected and appointed—may undervalue such normative commitments in structuring the concrete policy processes in which they participate. The good that may come from fulfilling these democratic commitments is likely to be felt only gradually and over a diffuse population. In the short-term, elected policy makers may well be focused primarily on their immediate political fortunes, while appointees seek to demonstrate the kinds of concrete progress in the achievement of immediate bureaucratic goals that will warrant continuing resource support adequate to meet near-term challenges on behalf of well-defined constituencies.

It is hard to imagine a time, however, in which the case for some "loftier," long-term thinking would be more urgent. Public confidence in governing institutions has never been lower, and the public's alienation from elected authorities never greater.[68] The outpouring of right and left-wing populist energy, embodied respectively in the Tea Party and Occupy movements, testifies eloquently to Americans' widespread cynicism about the capacities and motivations of governing elites.[69] Meaningful efforts to reconnect everyday citizens with their governing institutions are urgently required to reestablish public trust. In their absence, a wave of general anti-government sentiment may make it impossible for any agency, no matter how

---

[68] Lydia Saad, *Congress Ranks Last in Confidence in Institutions: Fifty percent "very little"/"no" confidence in Congress reading is record high*, GALLUP (July 22, 2010), http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx. Professor Lawrence Lessig puts the point dramatically:

> At what point do we declare an institution politically bankrupt, especially an institution that depends fundamentally upon public trust and confidence to do its work? When the czar of Russia was ousted by the Bolsheviks, he had the confidence of more than 11 percent of the Russian people. When Louis XVI was deposed by the French Revolution, he had the confidence of more than 11 percent of the French. And when we waged a Revolutionary War against the British Crown, more than 11 percent of the American people had confidence in King George III.

LAWRENCE LESSIG, REPUBLIC, LOST: HOW MONEY CORRUPTS CONGRESS—AND A PLAN TO STOP IT 247 (2011).

[69] Bruce Reyes-Chow, *The Tea Party and Occupy Wall Street Movements: Similarities and Differences*, HUFFINGTON POST (Nov. 1, 2011), http://www.huffingtonpost.com/bruce-reyeschow/tea-party-occupy-movement_b_1062824.html.

urgent its mission, to garner the public support necessary to do jobs that need doing. In the cyber realm, for example, there is credible "worry that cuts being mulled over by Congress and the White House could sink the nation's nascent cyber defenses."[70]

Cyber policy makers, moreover, ought to recognize that public participation in their domain may also furnish practical benefits that will enhance their mission, even in the relatively short term. Public participation can aid in agenda setting by clarifying the problems that need to be addressed and the priorities that ought to attach to them. The public may bring to decision makers' attention potential impacts of different policies that might not otherwise be considered, as well as information about the potential distribution of burdens and benefits. The perspective of outsiders might be especially useful in assessing the credibility of information that policy makers have gathered, and in testing the logic that, in the minds of policy makers, links potential policies to desired objectives. In the realm of environmental policy, the NRC, after an exhaustive review of available case studies and survey and experimental research, concluded that, on average, public participation enhances the quality and legitimacy of environmental decisions, as well as the capacity of both experts and the lay public to make better decisions in the future.[71] There is no obvious reason why the outcome should be different in the cyber realm, where the mix of fact and value inputs is similarly complex and positive impacts are likely to depend on the behaviors of multiple groups of actors, including private citizens.

The most intense objections from agency policy makers are likely to appear in the form of doubts as to the utility of deliberation with non-experts. In research I did in 2009 on early efforts by the current Federal Communications Commission (FCC) leadership to expand public input in FCC decision making,[72] a number of senior staff expressed genuine uncertainty as to the role non-expert opinion was supposed to play in their decision making. In the words of one staff member, "Aren't we supposed to be the expert agency? What's the general public going to tell me about the hard technical choices we

---

[70] Jennifer Martinez, *Balancing Act: Cybersecurity vs. Cuts*, POLITICO (Oct. 23, 2011, 10:12 PM), http://www.politico.com/news/stories/1011/66665.html.

[71] DIETZ & STERN, *supra* note 37, at 76.

[72] Peter M. Shane, *Empowering the Collaborative Citizen in the Administrative State: A Case Study of the Federal Communications Commission*, 65 U. MIAMI L. REV. 483, 485 (2011).

face that I do not already know?"[73] Such an objection, however, ignores two critical points. The first is that decision making confined to experts is prone to its own kinds of deficiencies. Happily, evidence does suggest that "experts are less likely to make certain sorts of predictable errors, such as overestimating the likely recurrence of vivid events, and more likely to gain some adaptive ability to overcome erroneous judgments as a result of repeat encounters with specific factual scenarios."[74] Experts, however:

> are subject to three distinct biases of their own. First, they are likely to overestimate their actual knowledge. In the experimental setting, they demonstrate levels of confidence in their judgments that exceed the actual advantages conferred by their expertise, the propensity to be "often wrong, but never in doubt." Second, they are likely to adopt a world view that turns largely on the area of their expertise and are unable to weigh its relative merits against other matters outside the zone of their expertise . . . Third, and relatedly, they are subject to routinized ways of approaching problems and to an unreflective "group think" style of inbred behavior.[75]

Melding expert analysis with broad-based deliberation can help offset each of these biases.

Indeed, public deliberation may be critical for countering the tendency among experts to pose problems solely within the technical frameworks with which they feel most comfortable. Whether to devote public resources to better firewalls, for example, or to various kinds of "workarounds" that would permit critical infrastructure to function even in the face of cyber aggression is a determination as likely to involve political, social, and economic tradeoffs as it is a technical assessment regarding the possible success of such strategies. So are decisions regarding our national doctrine on cyber war, investments in systems designed to improve cyber attribution, the allocation of cyber authority among military and civilian authorities, and the scope

---

[73] Private communication.

[74] Samuel Issacharoff, *Behavioral Decision Theory in the Court of Public Law*, 87 CORNELL L. REV. 671, 675 (2002).

[75] *Id.*

of presidential authority over the Internet. One does not have to impute ill motive to imagine how specialists in law, economics, military science, and information science might be tempted to characterize these issues as "ultimately" about legality, efficiency, operations research, or sound management. All of these disciplines are implicated, but so are public values regarding liberty, privacy, accountability, and competing priorities. These values should not be subordinated in the creation of public policy.

The second point is that good design for a policy process intended from the outset to accommodate non-expert policy input is quite likely to improve the quality of the relevant technical analysis as well. In studying the processes by which the public has been involved in environmental assessment and risk analysis more generally, the NRC has advanced five requisites for effectively "melding scientific analysis and public participation."[76] These are:

1. ensuring transparency of decision-relevant information and analysis,

2. paying explicit attention to both facts and values,

3. promoting explicitness about assumptions and uncertainties,

4. including independent review of official analyses and/or engaging in a process of collaborative inquiry with interested and affected parties, and

5. allowing for iteration to reconsider past conclusions on the basis of new information.[77]

Determined planning for the fourth of these steps—the actual stage of public participation—would appear to be an especially promising strategy for making sure the first three of these requirements are met. That is, the administrators in charge of organizing public input are likely to be strongly positioned to insist that the relevant teams of experts identify both the assumptions and sources of information that underlay their analyses, the degree of uncertainty that attends their

---

[76] DIETZ & STERN, *supra* note 37, at 3.

[77] *Id.*

conclusions, and the value questions to which their analyses are actually directed. This is a level of clarity likely to be of enormous help not only to the citizen-deliberators, but also to the agency policy makers to whom the experts are intended to be accountable. Technical analysis that meets these requirements is quite likely to be more thoughtful technical analysis.

There is no guarantee, of course, that a public participation project will yield these kinds of benefits. Certainly, there are public participation initiatives that have not been successful. But the design of the process is critical:

> The way a public participation process is conducted can have more influence on overall success than the type of issue, the level of government involved, or even the quality of preexisting relationships among the parties. Thus, those variables over which the convening agency has the greatest control turn out to be key to achieving the desired results.[78]

According to the NRC: "The evidence indicates that public participation processes have better results when they follow basic principles of program management: clarity of purpose, commitment, adequate resources, appropriate timing, an implementation focus, and a commitment to learning."[79] Beyond these basic principles, however, the experience of participation needs itself to be designed in a way most likely to elicit the payoffs most valuable in the policy domain at issue. Some version of deliberative polling, supported by an agency (or coalition of agencies) with both a clear sense of objectives and a willingness to commit explicitly "to supporting the process and taking seriously the results,"[80] seems tailor-made for connecting the public to public policy in the cyber realm.

V. CONCLUSION

The state of cybersecurity policy making in the United States is plainly unsatisfactory. Lines of decisional authority in the government are unclear. Adequate leverage over the management of private

---

[78] *Id.* at 95.

[79] *Id.* at 109.

[80] *Id.* at 99.

infrastructure is uncertain. The public is largely oblivious to the dimensions of the problem and the government's policy directions in response to it. It is unlikely that current laws are doing what needs to be done in terms of incentivizing responsible behavior on the part of those most able to shoulder the costs of improving security. As a consequence, the cyber realm appears well-characterized by Jeffrey Hunker as plagued by "creeping failure."[81] Cyberspace is not so linked (yet) with any catastrophic consequence as to motivate a concentrated public response and yet, day by day, year by year, it bears enormous social costs with the proliferation of cyber aggression, both criminal and political.

There is no particular reason for this situation to change unless an informed public is motivated around the issue of cybersecurity to help mobilize government in the direction of real solutions. Laden as it is with science and technology, the cyber realm may seem a daunting frontier on which to launch newly ambitious forms of public engagement, but its seeming obscurity may be an advantage, as well. That is, cybersecurity is not a subject on which citizens are likely to begin from a hugely polarized stance. Our racial, ethnic, gender, religious, and partisan identities are unlikely to be deeply implicated in cybsersecurity deliberations. Cyber may thus be an ideal realm around which the government could try to organize the citizenry into conversations, both with each other and with government, that truly deepen the experience of democratic citizenship.[82]

It is not as if agencies within our government have not already thought of this at some level. For example, on September 21, 2011, the Federal Register published a notice from the Departments of Commerce and Homeland Security requesting public comment on a voluntary industry code of conduct for notifying consumers when their computers have been used illicitly by botnets.[83] This is an excellent topic for citizen input. Following the close of the comment period, a visit to the online compendium of public responses revealed

---

[81] HUNKER, *supra* note 7, at 8.

[82] Stephen Coleman, *Making the E-Citizen: A Sociotechnical Approach to Democracy*, CONNECTING DEMOCRACY: ONLINE CONSULTATION AND THE FLOW OF POLITICAL COMMUNICATION 379 (Stephen Coleman & Peter M. Shane, eds., forthcoming Dec. 2012).

[83] *Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware*, 76 Fed. Reg. 58,466 (Sept. 21, 2011).

exactly nine submissions by the original November 4, 2011 deadline.[84] Only eighteen more comments[85] resulted from a ten-day extension of the comment period.[86] We know how to do democracy better than this. All that is required is will.

VI. APPENDIX: A SCENARIO FOR PUBLIC DELIBERATION

The April, 2009 White House Cyberspace Policy Review declares: "The United States needs to conduct a national dialogue on cybersecurity to develop more public awareness of the threat and risks and to ensure an integrated approach toward the Nation's need for security and the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law."[87] The most effective mechanism for galvanizing such a dialogue would be a blue-ribbon national commission, like the 9/11 Commission,[88] the Carnegie Commission that led to the creation of the Corporation for Public Broadcasting,[89] or the Kerner Commission[90] that looked into the causes of the 1960s' race riots in the United States. Assuming such a commission were either chartered by statute—the ideal situation—or organized as a federal advisory committee,[91] it would be perfectly situated to sponsor a deliberative poll on critical aspects of cyber

---

[84] *Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware: Comments received in Response to Federal Register Notice* 110829543–1541–01, NAT'L INST. OF STANDARDS AND TECH. (Nov. 21, 2011), http://www.nist.gov/itl/botnetcomments.cfm.

[85] *Id.*

[86] National Protection and Programs Directorate; Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware; Extension of Comment Period, 76 Fed. Reg. 68, 160 (Nov. 3, 2011).

[87] THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 1 (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[88] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U. S., THE 9/11 COMMISSION REPORT (2004).

[89] CARNEGIE COMM'N ON EDUCATIONAL TELEVISION, PUBLIC TELEVISION: A PROGRAM FOR ACTION (1967).

[90] NAT'L ADVISORY COMM'N ON CIVIL DISORDERS, REPORT OF THE NATIONAL ADVISORY COMMISSION ON CIVIL DISORDERS (1968).

[91] 5 U.S.C. app. § 2 (2006).

policy. The following is an outline of the organizational steps that would be entailed in staging that deliberative poll.

1. After doing its preliminary "environmental scan" of the relevant issues, the commission would frame the question or questions for public deliberation. Examples might be, "How much authority should rest with the Department of Defense for protecting civilian computer networks in the United States?" or, "How should the United States direct the investment of budgetary resources to advance the goals of cybersecurity?"

2. The commission would issue a request for proposals for a nonpartisan, nonprofit entity to serve as process consultant for the deliberative poll.

3. The consultant, in consultation with the commission, would assemble an advisory committee for the deliberative poll. The advisory committee would be selected to represent identifiable interests both within and outside government that could be significantly affected by new policy, and a wide range of political and philosophical perspectives. The key tasks of the advisory committee would be to select a diverse group of experts to participate in the deliberative poll and to vet the briefing materials to insure that each competing perspective on every question was presented fairly and to the satisfaction of its advocates.

4. The consultant, working with the commission, would develop a media plan to ensure widespread and in-depth coverage of the deliberative poll as it evolves. All materials prepared for the deliberative poll would be made available online, along with opportunities for members of the public to discuss those materials.

5. Under the consultant's supervision, a random sample of Americans would be surveyed on the questions on which the deliberative poll is focusing. The sample would be large enough to provide reasonable assurance that 300 volunteers would emerge from the group to engage in actual deliberations.

6. Every person who responds to the survey would be invited to participate in the deliberative poll. Because face-to-face deliberation is ideal, participants would be offered financial assistance to cover their travel and a small stipend for their work.

7. The deliberative poll would be conducted, presumably in Washington, D.C., over the course of a weekend. As is typical, participants would be organized into small groups on arrival and would deliberate initially on the adequacy of the briefing materials and questions left unanswered. Questions formulated by the groups would then be posed to the diverse panel of experts. Participants would then continue to deliberate in small groups, leading to a final, confidential survey of the participants.

8. Raw results of the poll would be announced immediately, while the consultant would commence preparing a detailed report summarizing highlights of the discussions and placing the results in context.

9. A public hearing of the commission would be convened following the submission of the final report, at which time the commission would formally respond to the poll's recommendations. In the intervening months, public television will have broadcast a documentary about the deliberations, newspapers, magazines, and blogs will have covered the issues extensively, and Congress would be gearing up for its own public hearings in response to the commission's recommendations.